이학박사 학위논문

Generalized Goldbach's Conjectures and the Arithmetic of Elliptic Curves

(일반화된 골드바흐 추측과 타원 곡선의 산술에 관하여)

2018년 2월

서울대학교 대학원

수리과학부

정근영

Generalized Goldbach's Conjectures and the Arithmetic of Elliptic Curves

(일반화된 골드바흐 추측과 타원 곡선의 산술에 관하여)

지도교수 변동호

이 논문을 이학박사 학위논문으로 제출함

2017년 10월

서울대학교 대학원

수리과학부

정근영

정근영의 이학박사 학위논문을 인준함

2017년 12월

위 원 장 _____ (인)

부 위 원 장 _____ (인)

위 원 _____ (인)

위 원 _____ (인)

위 원 _____ (인)

Generalized Goldbach's Conjectures and the Arithmetic of Elliptic Curves

A dissertation
submitted in partial fulfillment
of the requirements for the degree of
Doctor of Philosophy
to the faculty of the Graduate School of
Seoul National University

by

Keunyoung Jeong

Dissertation Director : Professor Dongho Byeon

Department of Mathematical Science
Seoul National University

February 2018

Abstract

Generalized Goldbach's Conjectures and the Arithmetic of Elliptic Curves

Keunyoung Jeong

Department of Mathematical Sciences
The Graduate School
Seoul National University

In this thesis, we introduce a totally new method which constructs integral points of elliptic curves. The main idea is that results on the theory of exceptional sets of linear type generalizations of strong Goldbach conjecture show the existence of integral points of certain elliptic curves, which are called cubic twists.

We first show that the size of exceptional sets of linear type generalizations of strong Goldbach conjecture is relatively small by generalizing previous works. We also explain why this result can be used for constructing integral points of elliptic curves. After that we give two applications about the theory of elliptic curves. One is that there are infinitely many sums of two rational cubes which have arbitrary number of prime divisors. The other is that under the parity conjecture, there are infinitely many elliptic curves whose Mordell–Weil groups are exactly $\mathbb{Z} \times \mathbb{Z}$.

Key words: Elliptic curves, Cubic twists, Mordell–Weil group, Goldbach's conjecture, Circle method.
Student Number: 2012-20255

Contents

Chapter 1

Introduction

In number theory, one of the main problem is to find rational solutions of Diophantine equations. For Diophantine equations which define algebraic curves, there is an invariant which is called a genus. It plays an important role in the theory of Diophantine geometry; When the genus is zero, the corresponding algebraic curve is essentially the projective line $\mathbb{P}^1$, thus the problem is relatively easy. The famous theorem of Falting shows that when a genus of a curve is 2 or more, then the number of rational points of the curve is finite. For the last case, when the genus is one, the curve is an elliptic curve or its twist. The elliptic curve is one of the main objects of this dissertation.

On the other side, there are also important problems in additive number theory. Goldbach conjecture and Waring problems are famous examples in this theory. Hardy, Littlewood, and Vinogradov established and developed the circle method to attack these conjectures. In Chapter 2, we will give a brief introduction to a circle method and an elliptic curve.

The main theme of this dissertation is generating rational points of elliptic curve, by using an analytic circle method. First, we show that an exceptional set of certain linear type generalizations of Goldbach conjecture is small in Chapter 3. The main theorem in Chapter 3 shows the existence of non-trivial integral points of a family of elliptic curves. This phenomenon has applications

in the arithmetic of elliptic curves. In this dissertation, we give two examples. In Chapter 4, we will show that there are infinitely many integers which are sum of two rational cubes, and have many prime divisors. In Chapter 5, under the parity conjecture, we construct elliptic curves whose rational points form an abelian group $\mathbb{Z} \times \mathbb{Z}$.

All results in this dessertation are already published. The results in Chapter 3 and 4 is in [BJ17], and the result of Chapter 5 is in [BJ16].

Chapter 2

Preliminaries

2.1 Circle method

In this section, we introduce history, basic settings, and ideas of Hardy–Littlewood circle method. The literatures [Vau, Chapter 1, 2], [Hel, Introduction] handle these topics. The circle method was invented to estimate the number of integer, or prime solutions of given equations. For example, Waring asserted that an equation

$$n = m_1^k + m_2^k + \cdots + m_s^k, \qquad m_i \in \mathbb{N}$$

always has a solution where s is greater than some number $s(k)$, depends only on k. In other words, he believed that for arbitrary natural number k there exists an s such that every natural number n can be represented by a sum of at most s k-th power of natural numbers.

Another example is Goldbach conjecture, which claims that equations

$$2n = p_1 + p_2, \qquad 2m + 1 = q_1 + q_2 + q_3$$

have solution in the set of primes for all natural number $n, m \geq 3$.

The exponential sum is useful tool to study such problems for the representation of numbers. Let $\mathcal{A} = (a_n)$ be a strictly increasing sequence of

non-negative integers, and

$$F(z) = \sum_{i=1}^{\infty} z^{a_m}, \qquad |z| < 1.$$

Then, the n-th coefficient of s-the power of $F(z)$ is the number of representation of n as a sum of s-elements in $\mathcal{A}$. For large n, by Cauchy's integral formula we can estimate it by computing

$$\frac{1}{2\pi i} \int_C F(z)^s z^{-n-1} dz$$

where C is a non-trivial circle centered at 0 of radius less than 1. This is an idea of Hardy and Littlewood. Later Vinogradov introduced some refinements. We use abbreviation $e(n) = e^{2\pi i n}$. Then there is a trivial orthogonality relation

$$\int_0^1 e(x\alpha) d\alpha = \begin{cases} 1 & \text{if } x = 0, \\ 0 & \text{if } x \neq 0. \end{cases}$$

For equations $g(x, y)$, a subset of natural numbers $\mathcal{A}$, and $\mathcal{A}(X) = \{x \in \mathcal{A} : x \leq X\}$,

$$\sum_{m,n \in \mathcal{A}(X)} \sum \int_0^1 e(g(m,n)\alpha) d\alpha \tag{2.1}$$

is the number of solutions $m, n \in \mathcal{A}(X)$ satisfying $g(m, n) = 0$. Hence to find the number of zeros of the equation g, it is enough to evaluate the integral of exponential sums.

The idea for the evaluation of such integrals is dividing an interval $[0, 1]$ into two parts - the major arc, and the minor arc. Let X be a large number, P be a X^δ for some small δ, $\mathfrak{M} \subset [0, 1]$ be the *major arc* defined by

$$\mathfrak{M} = \bigcup_{\substack{0 \leq a \leq q \leq P \\ (a,q)=1}} \mathfrak{M}(q, a),$$

where

$$\mathfrak{M}(q, a) = \left\{ \alpha \in [0, 1] : \left| \alpha - \frac{a}{q} \right| \leq \frac{P}{qX} \right\}$$

and $\mathfrak{m} \subset [0,1]$ be the *minor arc* defined by

$$\mathfrak{m} = [0,1] \setminus \mathfrak{M}.$$

In other words, the major arc is a set of elements which are close to the rational numbers. The integral (2.1) is divided into two parts,

$$\int_{\mathfrak{m}} \sum_{m,n \in \mathcal{A}(X)} \sum e(g(m,n)\alpha) d\alpha + \int_{\mathfrak{M}} \sum_{m,n \in \mathcal{A}(X)} \sum e(g(m,n)\alpha) d\alpha. \tag{2.2}$$

The advantage of this approach is followed by Dirichlet's approximation theorem.

Theorem 2.1 (Dirichlet)**.** *Let α be a real number. Then, for each $N \geq 1$ there exists a rational number $\frac{a}{q}$ such that $(a,q) = 1$, $1 \leq q \leq N$, and*

$$|\alpha - \frac{a}{q}| \leq \frac{1}{qN}.$$

For any real nubmer α and $N = \frac{X}{P}$, there exists $q \leq N$ such that $|\alpha - \frac{a}{q}| \leq \frac{P}{qX}$. Therefore if α is in a minor arc, then q is greater than P. It gives the upper bound of the minor arc part in (2.2) in the two examples which are dealt at the start of this chapter, by the terms of X and q. On the other hand, the major arc part in (2.2) is

$$\sum_{a,q} \int_{-\frac{P}{qX}}^{\frac{P}{qX}} \sum_{m,n \in \mathcal{A}(X)} \sum e(g(m,n)(\frac{a}{q} + \eta)) d\eta.$$

When the case is sufficiently nice, we can calculate these terms since α is close to the rational numbers.

We did not prove anything in this chapter, but this strategy gives results on both problems - Waring problem and Goldbach's conjecture. In [Vau, Chpater 2] one can find the proof of $s(k) < 2^k + 1$, following the story of this chapter. In [BKW00] the authors gave the bound of the exceptional set of Goldbach's conjecture. We will talk about the exceptional set of certain linear type generalization of Goldbach's conjecture in Chapter 3.

2.2 Elliptic curves

The goal of this section is to introduce basic properties of elliptic curves, Birch and Swinnerton-Dyer conjecture, and the parity conjecture. All results in this section are not original; they are treated in numerous literatures, like [Sil09], [Sil94], [Cas65], and [Kob]. For the proof of theorems in this section, we will give a precise reference.

Definition. A projective algebraic curve of genus 1 with a distinguished rational point is called an elliptic curve.

Let us denote an elliptic curve by E, and its base field by K. As in [Har, Proposition IV.4.6], every elliptic curve can be embeded in $\mathbb{P}^2$ with a projective equation

$$Y^2Z + a_1XYZ + a_3YZ^2 = X^3 + a_2X^2Z + a_4X^2Z + a_6Z^3,$$

where $a_i \in \overline{K}$ for all i. There is at least one rational point $[0, 1, 0]$. When one takes an affine equation, it is replaced by

$$y^2 + a_1xy + a_3y = x^3 + a_2x^2 + a_4x^2 + a_6.$$

This equation is called a Weierstrass equation, and defined over K if all coefficient a_i is in the field K. When the characteristic of base field K is not 2 or 3, we can simplify this equation by some change of variables, yielding

$$y^2 = x^3 + ax + b, \qquad \text{for } a, b \in \overline{K}.$$

We define the discriminant and the j-invariant of this equation, denoted by Δ_E, and j_E as a $\Delta_E = -16(4a^3 + 27b^2)$, and $j_E = -1728\frac{(4a)^3}{\Delta_E}$, respectively.

Proposition 2.2. *A curve given by a Weierstrass equation $y^2 = x^3 + ax + b$ is an elliptic curve if and only if $\Delta_E \neq 0$. Two elliptic curves defined by Weierstrass equations are isomorphic if and only if their j-invariants are same.*

Proof. [Sil09, Proposition III.1.4]. □

Since an elliptic curve is isomorphic to its Jacobian, there is a natural abelian group structure with an identity element at infinity. (cf. [Sil09, Proposition III.3.4]) Let us define a morphism in the category of elliptic curves.

Definition. An isogeny between algebraic groups is a morphism which is a surjective and has a finite kernel.

When the algebraic groups are elliptic curves, a map is an isogeny if and only if it is regular and preserves identity. The only if part is trivial, and the converse is deduced by following two theorems:

Theorem 2.3. *A morphism between two projective nonsingular curves is surjective, or a constant.*

Proof. [Har, Proposition II.6.8]. □

Theorem 2.4. *A regular map between elliptic curves which preserves identity, also preserves the additive structure.*

Proof. [Sil09, Theorem III.4.8]. □

A simple example of an isogeny is a multiplication by n, which maps a point $P \in E$ to $nP = P + \cdots + P \in E$. (cf. [Sil09, Proposition III.3.6]). Therefore, there is a natural inclusion $\mathbb{Z} \longrightarrow \mathrm{End}\, E$. This map is usually surjective. Unless, we say that an elliptic curve E has *complex multiplication*.

The theorem of Mordell, which was generalized by Weil, shows that the rational points of elliptic curves form a finitely generated abelian group.

Theorem 2.5. *Let E be an elliptic curve over a field K. Then, there is a group structure on the set of K-rational points of E. Moreover, this group is a finitely generated abelian group.*

Proof. [Sil09, Chapter VIII]. □

An abelian group of a K-rational points of E is usually denoted by $E(K)$, and called a Mordell–Weil group of E over K. The notations $E(K)_{\mathrm{tors}}, r_E$ indicate the torsion subgroup, and the rank of $E(K)$, respectively. When the base field is the set of rational numbers, the result of Mazur [Maz77] showed that there are only 15 groups which is a torsion subgroup of $E(\mathbb{Q})$. In practice, the theorem of Nagell–Lutz effectively computes the torsion subgroup of $E(K)$. Hence in the view of Diophantine equation, the hardest part is computing the rank of Mordell–Weil group. We will introduce the effective way to calculate the upper bound of rank of the Mordell–Weil groups.

Let K be a field, v be a place of K, $H^1(G_K, \cdot)$ be a first cohomology of Galois module $(\cdot)$, and loc_v be a localization map induced by a fixed embedding $i : K \longrightarrow K_v$.

Definition. For a prime number p, the p-Selmer group of an elliptic curve E over K is a kernel of $i_* \circ \oplus_v \mathrm{loc}_v = \oplus_v \mathrm{loc}_v \circ i_*$, where

$$\begin{array}{ccccccccc} 0 & \longrightarrow & \frac{E(K)}{pE(K)} & \longrightarrow & H^1(G_K, E[p]) & \xrightarrow{i_*} & H^1(G_K, E)[p] & \longrightarrow & 0 \\ & & \downarrow & & \downarrow{\scriptstyle \oplus \mathrm{loc}_v} & & \downarrow{\scriptstyle \oplus \mathrm{loc}_v} & & \\ 0 & \longrightarrow & \bigoplus_v \frac{E(K_v)}{pE(K_v)} & \longrightarrow & \bigoplus_v H^1(G_{K_v}, E[p]) & \xrightarrow{i_*} & \bigoplus_v H^1(G_{K_v}, E)[p] & \longrightarrow & 0 \end{array}$$

We define a Shafarevich–Tate group of an elliptic curve over number field K, denoted by $Ш(E/K)$, as a kernel of

$$\oplus \mathrm{loc}_v : \ H^1(G_K, E) \longrightarrow \bigoplus_v H^1(G_{K_v}, E).$$

A part of Birch–Swinnerton-Dyer conjecture predicts that the $Ш(E/K)$ is finite for all elliptic curves and the number field K. The result of Rubin [Rub87] and Kolybagin [Kol89] handle some cases, however, for general cases it remains open. On the other hand, the finiteness of Selmer groups is relative elementary.

Theorem 2.6. *For all elliptic curves E/K and prime p, the p-Selmer group $\mathrm{Sel}_p(E/K)$ is finite.*

Proof. [Sil09, Theorem X.4.2]. □

The theory of descent effectively calculates the size of Selmer groups of an elliptic curve. (cf. [Sto]) By the exact sequence in the above definition,

$$0 \longrightarrow \frac{E(K)}{pE(K)} \longrightarrow \mathrm{Sel}_p(E/K) \longrightarrow Ш(E/K)[p] \longrightarrow 0$$

is exact. Therefore, the $\mathbb{F}_p$-dimension of Selmer groups gives an upper bound of the rank of the weak Mordell–Weil group of elliptic curves.

To study a Selmer group of an elliptic curve, it is essential to study an elliptic curve over local fields K_v since in the diagram in Definition 2.2, there are cohomology groups of an elliptic curve over local fields. Let O_{K_v} be a ring of integer of local field K_v, π be a uniformizer of O_{K_v}, and k_v be a residue field $O_{K_v}/\pi O_{K_v}$. We also assume that k_v is always finite.

When we choose a minimal Weierstrass equation of elliptic curves, the natural reduction map $O_{K_v} \longrightarrow k_v$ induces a reduction map on the elliptic curve

$$E \longrightarrow \widetilde{E}.$$

Note that $\widetilde{E}$ a curve defined over k_v is possibly singular. When $\widetilde{E}$ is singular, the non-singular part of $\widetilde{E}$ which is denoted by $\widetilde{E}^{\mathrm{ns}}$ forms an abelian group. (cf. [Sil09, Proposition 2.5])

Definition. Let E be an elliptic curve over a local field K_v, and $\widetilde{E}$ be a reduction modulo π of a minimal Weierstrass equation of E. Then, we define

$$E_0(K_v) = \left\{ P \in E(K_v) : \widetilde{P} \in \widetilde{E}^{\mathrm{ns}}(k_v) \right\}, \quad E_1(K_v) = \left\{ P \in E(K_v) : \widetilde{P} = O \right\}.$$

Definition. (a) E has good reduction at v if $\widetilde{E}$ is nonsingular over k_v.

(b) E has split multiplicative reduction if $\widetilde{E}$ has a node, and the slopes of the tangent lines at the node are in k_v.

(c) E has non split multiplicative reduction if $\widetilde{E}$ has a node, and one of the slopes of the tangent lines at the node is not in k_v.

(d) E has additive reduction at v if $\widetilde{E}$ has a cusp.

The rank of Mordell–Weil group is sometimes called an "algebraic rank" of the elliptic curve, since the Mordell–Weil group is an algebraic object related to an elliptic curve. On the other hand, there is a notion of the analytic rank of the elliptic curves. We first introduce an analytic object related to elliptic curves.

Definition. The L-function of an elliptic curve E is

$$L(s,E) = \prod_{p \nmid \Delta_E} \frac{1}{1 - a_p(E)p^{-s} + p^{1-2s}} \cdot \prod_{p|\Delta_{E,1}} \frac{1}{1-p^{-s}} \cdot \prod_{p|\Delta_{E,2}} \frac{1}{1+p^{-s}},$$

where $a_p(E) = p + 1 - \#\widetilde{E}(\mathbb{F}_p)$, $\#\widetilde{E}(\mathbb{F}_p)$ the number of $\mathbb{F}_p$-point of $\widetilde{E}$, $\Delta_{E,1}$ a product of primes of which E has split multiplicative reduction, and $\Delta_{E,2}$ a product of primes of non split multiplicative reduction.

There are natural questions to the L-function - about convergency, analytic continuation, and functional equations. When the base field is the rational number, the modularity theorem, which was first proved by [Wil95] for semistable elliptic curves and by [BCDT01] for all elliptic curves, shows that an L-function of an elliptic curves coincides to an L-function of a modular form f_E. Therefore it has an analytic continuation and a functional equation. For a general number field K, there is an *automorphic conjecture*, which claims that an L-function of an elliptic curve over K agrees with an L-function of a cuspical automorphic representation of GL_2 up to normalization. It is proved for the real quadratic extensions, in [FHS15].

When E is defined over $\mathbb{Q}$, we write a functional equation concretely. Let $\Gamma(s)$ be a usual gamma function, defined by $\int_0^\infty t^{s-1}e^{-t}dt$.

Proposition 2.7. *Let E be an elliptic curve defined over $\mathbb{Q}$. Then, a function $\Lambda(s,E) = N_E^{s/2}(2\pi)^{-s}\Gamma(s)L(s,E)$ has a functional equation*

$$\Lambda(s,E) = \omega_E \Lambda(2-s,E),$$

where $\omega_E \in \{\pm 1\}$ which is called the root number of E.

Proof. By the modularity theorem over $\mathbb{Q}$ [BCDT01] and [Kob, p.142, Weil's theorem]. □

The order of zero of $L(s,E)$ at $s=1$ is called the *analytic rank* of E. A part of Birch and Swinnerton-Dyer conjecture claims that

$$r_E = \mathrm{ord}_{s=1} L(s,E).$$

There are various results of this conjecture, when the rank of E is equal or less than one. Gross and Zagier [GZ86] show that when an analytic rank of E is one, an algebraic rank of E is at least one. Kolyvagins [Kol89] strengthens this result. He shows that if the analytic rank of E is zero or one, then the algebraic rank is also zero or one. However, there is no one example of elliptic curve E satisfying Birch and Swinnerton-Dyer conjecture and $\mathrm{rank}(E(K)) \geq 2$.

By Proposition 2.7, the parity of root number of E is equal to the parity of the order of zero of the L-function. In other words, $\omega_E = (-1)^{\mathrm{ord}_{s=1}L(s,E)}$. We get the following another conjecture, which is weaker than the Birch and Swinnerton-Dyer conjecture.

Conjecture 2.8 (Parity conjecture)**.** Let E be an elliptic curve and r_E be its rank. Then a parity of rank of E is equal to $\omega_E \in \{\pm 1\}$, a root number of E. In other words,

$$(-1)^{r_E} = \omega_E.$$

In some cases, an explicit calculation of the root numbers are already known. (cf. [BS66], [Con94].) A part of the Birch and Swinnerton-Dyer conjecture, which is the finiteness of the Shafarevich–Tate group of elliptic curves

implies that the parity conjecture. It is proved by Dokchitser and Dokchitser [DD11].

We will study how the calculation of root number can be used for the existence of the rational point under the parity conjecture. If one can prove that the root number of certain elliptic curves with a trivial torsion subgroup is -1, then under the parity conjecture this elliptic curve have a rational point. Similarly if an elliptic curve with root number $+1$ has at least one rational point which is not a torsion point, then its rank is at least two. This idea will be used in Chapter 5.

Chapter 3

Exceptional set of Goldbach's problem

3.1 Main theorem

One of the prominent problems in additive number theory is Goldbach conjecture. The main strategy for this problem is a circle method, which was first studied by Hardy and Littlewood. Vinogradov proved weak Goldbach's conjecture for large odd numbers in [Vin37]. This method also established that almost all even integers satisfy Goldbach's conjecture. Subsequent results studied more sharper estimates for the exceptional set of strong Goldbach's conjecture, like [MV75].

In [BKW00], the authors prove a quantitative strengthening of a theorem of Perelli [Per96]. Let $f(x) \in \mathbb{Z}[x]$ be a polynomial of degree k with a positive leading coefficient, and $\mathcal{S}(N, f)$ be the number of natural numbers $1 \leq n \leq N$, for which the equation

$$2f(n) = p_1 + p_2$$

does not have a solution in prime p_1 and p_2. Then, the authors showed that

Theorem 3.1 ([BKW00], Theorem 1)**.** *There is an absolute constant c such that*

$$\mathcal{S}(N, f) \ll N^{1-\frac{c}{k}}.$$

We consider a linear type generalization of Goldbach's problem under the restriction of residue classes on primes. In other words, we want to show that almost all elements of the polynomial sequence $\{f(n)\}_{n\in\mathbb{N}}$ can be represented by

$$2f(n) = Ap_1 + Bp_2, \qquad \text{for } p_1 \equiv i, p_2 \equiv j \pmod{g}.$$

Unfortunately, this analogue of Theorem 3.1 does not hold for all integers A, B, i, j, since if there is a congruence relation among f, A and B modulo g, then an exceptional set could be a whole set of natural numbers. For example, when $f(x) = 3x$, $A = B = i = j = 1$, and $g = 3$,

$$6n = p + q, \quad \text{for } p, q \equiv 1 \pmod{3}$$

does not have an integer solution. In this case the exceptional set is a set of natural numbers, so it is not less than $N^{1-\epsilon}$ for any real ϵ. Therefore, for the generalization of Theorem 3.1, we need certain reasonable conditions on the f, A, B, i and j, modulo g.

Theorem 3.2. *Let $f(x) \in \mathbb{Z}[x]$ be a polynomial which has a positive leading coefficient with degree k. Let A, B be relatively prime odd integers and i, j positive integers with $0 < i, j < g$ and $(i, g) = (j, g) = 1$. Suppose that there is at least one integer m such that*

$$2f(m) \equiv Ai + Bj \pmod{g} \text{ and } (AB, 2f(m)) = 1.$$

Let $\mathcal{S}_k^{ABij}(N, f)$ be the number of positive integers $n \in [1, N]$ with $2f(n) \equiv Ai + Bj \pmod{g}$ and $(AB, 2f(n)) = 1$ for which the equation $2f(n) = Ap_1 + Bp_2$ has no solution in primes $p_1 \equiv i, p_2 \equiv j \pmod{g}$. Then there is an absolute constant $c > 0$ such that

$$\mathcal{S}_k^{ABij}(N, f) \ll_f N^{1-\frac{c}{k}}.$$

Now we briefly explain why this theorem is a generalization of Theorem 3.1. Especially when $A = B = 1$,

$$\mathcal{S}(N, f) \cap \{1 \leq n \leq N : 2f(n) \equiv i + j \pmod{g}\} \subset \mathcal{S}^{11ij}(N, f).$$

Therefore

$$\mathcal{S}(N, f) \subset \bigcup_{i,j} \mathcal{S}^{11ij}(N, f),$$

which shows that Theorem 3.2 gives Theorem 3.1. In this sense Theorem 3.2 is a generalization of Theorem 3.1, which is a result on an exceptional set of Goldbach conjecture.

By Theorem 3.2, one can directly prove that there are infinitely many integers n such that

$$2f(n) = Ap_1 + Bp_2,$$

for some primes $p_1 \equiv i$ and $p_2 \equiv j \pmod{g}$ under the same conditions on A, B, i and g.

In the rest of this chapter, we use following notations: let N be a large positive integer, δ be a sufficiently small positive real number to be chosen later, $X = 2f(N)$, $P = X^{6\delta}$, $Q = X/P$ and $\kappa = 2^{-\frac{1}{k}}$. We define the exponential sum $S_i(\alpha)$ by

$$S_i(\alpha) = \sum_{\substack{P < p \leq X \\ p \equiv i \pmod{g}}} (\log p) e(\alpha p),$$

where $e(\alpha p) = e^{2\pi\alpha p i}$ and the summation is over primes p with $P < p \leq X$ and $p \equiv i \pmod{g}$. When $T \subseteq [0, 1]$, we put

$$r_{ABij}(n; T) = \int_T S_i(A\alpha) S_j(B\alpha) e(-\alpha n) d\alpha,$$

and $r_{ABij}(n) = r_{ABij}(n; [0, 1])$. Then $r_{ABij}(2f(n))$ counts the number of solutions of the equation $2f(n) = Ap_1 + Bp_2$ in primes $p_1 \equiv i$, $p_2 \equiv j \pmod{g}$ with weight $\log p_1 \log p_2$. Let $\mathfrak{M} \subset [0, 1]$ be the major arc defined by

$$\mathfrak{M} = \bigcup_{\substack{0 \leq a \leq q \leq P \\ (a,q)=1}} \mathfrak{M}(q, a),$$

where

$$\mathfrak{M}(q,a) = \left\{ \alpha \in [0,1] : \left| \alpha - \frac{a}{q} \right| \leq \frac{P}{qX} \right\},$$

and $\mathfrak{m} \subset [0,1]$ the minor arc defined by

$$\mathfrak{m} = [0,1] \setminus \mathfrak{M}.$$

3.2 Minor arc

The goal of this section is to evaluate a sum of $r_{ABij}(n;\mathfrak{m})$'s. We first note that the orthogonality relation of characters simplifies the sum $S_i(A\alpha)$. Let χ be a Dirichlet character of modulus g. The orthogonality relations of Dirichlet characters are

$$\sum_{\chi} \bar{\chi}(i)\chi(p) = \varphi(g)\delta(i,p),$$

where the sum is over all Dirichlet characters of modulus g, and

$$\delta(i,p) = \begin{cases} 1 & \text{if } p \equiv i \pmod{g}, \\ 0 & \text{if } p \not\equiv i \pmod{g}. \end{cases}$$

It implies that

$$\begin{aligned} S_i(A\alpha) &= \sum_{P<p\leq X} \frac{1}{\varphi(g)} \sum_{\chi} \bar{\chi}(i)\chi(p)(\log p)e(\alpha Ap) \\ &\ll \sum_{\chi} \left| \sum_{P<p\leq X} \chi(p)(\log p)e(\alpha Ap) \right|. \end{aligned}$$

This sum was first studied by [BP85], but we refine the proof of [IK, Theorem 13.6].

Lemma 3.3. *Let A, g be integers. Suppose that there exist a, q such that $(a,q) = 1$, $q \leq X$ and $\left|\alpha - \frac{a}{q}\right| \leq \frac{1}{q^2}$. Then*

$$S_i(A\alpha) = \sum_{\substack{p\leq X \\ p\equiv i \pmod{g}}} (\log p)e(\alpha Ap) \ll (X^{\frac{4}{5}} + Xq^{-\frac{1}{2}} + X^{\frac{1}{2}}q^{\frac{1}{2}})(\log X)^3.$$

Proof. We define the von Mangoldt function and its refinement, by

$$\Lambda(n)=\begin{cases}\log p & \text{if } n=p^k \text{ for some } k,\\ 0 & \text{otherwise,}\end{cases}\qquad \Lambda_A(n)=\begin{cases}\Lambda(\frac{n}{A}) & \text{if } A|n,\\ 0 & \text{otherwise.}\end{cases}$$

Let us use $\sum_{n\le X}\Lambda_A(n)e(\alpha n)$ to estimate the upper bound of $\sum_{p\le X}(\log p)e(\alpha Ap)$. Since

$$\sum_{p\le X}\chi(p)(\log p)e(\alpha Ap)=\sum_{n\le X}\chi(n)\Lambda(n)e(\alpha An)+O(\sqrt{X}),$$

$$S_i(A\alpha)\ll\sum_{\chi}\left|\sum_{p\le X}\chi(p)(\log p)e(\alpha Ap)\right|=\sum_{\chi}\left|\sum_{n\le AX}\chi(\frac{n}{A})\Lambda_A(n)e(\alpha n)\right|+O(\sqrt{X}). \tag{3.1}$$

Note that [IK, Proposition 13.4] with some modifications, we know that for all y and (n,A) satisfying $A|n$ and $\frac{n}{A}>z$,

$$\Lambda(\frac{n}{A})=\sum_{\substack{b|\frac{n}{A}\\ b\le y}}\mu(b)\log\frac{n}{Ab}-\sum_{\substack{bc|\frac{n}{A}\\ b\le y,c\le z}}\sum\mu(b)\Lambda(c)+\sum_{\substack{bc|\frac{n}{A}\\ b>y,c>z}}\sum\mu(b)\Lambda(c).$$

Then the term (3.1) is

$$\begin{aligned}\sum_{n'\le AX}\chi(\frac{n'}{A})\Lambda_A(n')e(\alpha n')&=\sum_{\substack{n'\le AX\\ A|n'}}\chi(\frac{n'}{A})\Lambda(\frac{n'}{A})e(\alpha n')\\ &=\sum_{\substack{lm\le AX\\ m<M,A|l}}\sum\chi(\frac{l}{A}m)\mu(m)\log\frac{l}{A}e(\alpha lm)\qquad(l=\frac{n'}{m}) &(3.2)\\ &\quad-\sum_{\substack{lmn\le AX,A|l\\ m\le M,n\le N}}\sum\sum\chi(\frac{l}{A}mn)\mu(m)\Lambda(n)e(\alpha lmn)\qquad(l=\frac{n'}{mn}) &(3.3)\\ &\quad+\sum_{\substack{lmn\le AX,A|l\\ m\le M,n\le N}}\sum\sum\chi(\frac{l}{A}mn)\mu(m)\Lambda(n)e(\alpha lmn)\qquad(l=\frac{n'}{mn}). &(3.4)\end{aligned}$$

For equations (3.2) and (3.3), we use the inequality

$$\sum_{1\le m\le M}\left|\sum_{\substack{mn\le X\\ A|n}}\chi(\frac{n}{A})e(\alpha mn)\right| \ll (M+\frac{X}{q}+q)\log qX, \tag{3.5}$$

which can be directly proven as in the proof of [IK, Proposition 13.6]. For (3.2),

$$\begin{aligned}&\sum_{m<M}\chi(m)\mu(m)\sum_{\substack{lm\le AX\\ A|l}}\chi(\frac{l}{A})\log\frac{l}{A}e(\alpha lm)\\ &\quad=\sum_{m<M}\chi(m)\mu(m)\int_1^{\frac{AX}{m}}\sum_{\substack{\gamma<l\le\frac{AX}{m}\\ A|l}}\chi(\frac{l}{A})e(\alpha ml)\frac{d\gamma}{\gamma}\\ &\quad-2\sum_{m<M}\chi(m)\mu(m)\sum_{\substack{lm\le AX\\ A|l}}\chi(\frac{l}{A})(\log A)e(\alpha lm).\end{aligned}$$

By applying

$$\sum_{\substack{y\le a\\ A|y}}f(y)\log\frac{y}{A}=\int_1^a\sum_{\substack{\gamma\le y\le a\\ A|y}}f(y)\frac{d\gamma}{\gamma},\qquad \sum_{\substack{\gamma<n\le\frac{X}{m}\\ A|n}}\chi(\frac{n}{A})e(\alpha mn)\ll\min(\frac{X}{m}-\gamma,\frac{1}{2\|\alpha mA\|}),$$

We have

$$\begin{aligned}&\sum_{m<M}\chi(m)\mu(m)\sum_{\substack{lm\le AX\\ A|l}}\chi(\frac{l}{A})\log\frac{l}{A}e(\alpha lm)\\ &\ll\left|\sum_{m<M}\mu(m)\chi(m)\int_1^{\frac{AX}{m}}\min(\frac{X}{m},\frac{1}{2\|\alpha mA\|})\frac{d\gamma}{\gamma}\right|+\sum_{m<M}\left|\sum_{\substack{lm<AX\\ A|l}}\chi(\frac{l}{A})e(\alpha lm)\right|\\ &\ll(M+\frac{X}{q}+q)(\log qX)\log X.\quad\because(3.5)\end{aligned}$$

Let us turn to (3.3).

$$\begin{aligned}
&\Big|\sum_{\substack{lmn\le AX, A|l\\ m\le M, n\le N}}\sum\sum\chi(\frac{l}{A}mn)\mu(m)\Lambda(n)e(\alpha lmn)\Big| \\
&\quad\le \left|\sum_{t\le MN}\sum_{\substack{tl\le X\\ A|l}}\log t\chi(\frac{l}{A}t)e(\alpha lt)\right| \le \log MN\sum_{t\le MN}\Big|\sum_{\substack{l\le \frac{AX}{t}\\ A|l}}\chi(\frac{l}{A})e(\alpha lt)\Big| \\
&\quad\ll (MN+\frac{AX}{q}+q)(\log 2qAX)\log MN \qquad \because (3.5) \\
&\quad\ll (MN+\frac{X}{q}+q)\log qX\log MN.
\end{aligned}$$

On the other hand,

$$\begin{aligned}
&\sum_{\substack{lmn\le AX, A|l\\ m>M, n>N}}\sum\sum\chi(\frac{l}{A}mn)\mu(m)\Lambda(n)e(\alpha lmn) = \sum_{\substack{mk\le AX\\ m>M\ k,n>N\\ A|\frac{k}{n}}}\sum\sum\chi(m\frac{k}{A})\mu(m)\Lambda(n)e(\alpha km) \\
&\quad= \sum_{m>M}\mu(m)\chi(m)\sum_{N<k\le\frac{AX}{m}}\sum_{n|\frac{k}{A}, n>N}\Lambda(n)\chi(\frac{k}{A})e(\alpha km) \\
&\quad= \sum_{m>M}\mu(m)\chi(m)\sum_{N<k\le\frac{AX}{m}}c_k\chi(\frac{k}{A})e(\alpha km) \qquad (c_k=\sum_{n|\frac{k}{A}, n\ge N}\Lambda(n)\ll\log k) \\
&\quad\ll \log X\sum_{\substack{mk\le AX\\ m>M, k>N}}\sum\mu(m)\chi(m)\chi(\frac{k}{A})e(\alpha km).
\end{aligned}$$

Again by (3.5) the last term is bounded by

$$(\frac{X}{M^{1/2}}+\frac{X}{N^{1/2}}+\frac{X}{q^{1/2}}+X^{1/2}q^{1/2})(\log X)^3.$$

We take $M=N=X^{\frac{2}{5}}$. Then

$$(3.2)\ll (X^{\frac{2}{5}}+\frac{X}{q}+q)\log qX\cdot\log X,$$

$$(3.3) \ll (X^{\frac{4}{5}} + \frac{X}{q} + q)\log qX \cdot (\log X)^3,$$
$$(3.4) \ll (X^{\frac{4}{5}} + Xq^{-1/2} + X^{1/2}q^{1/2})(\log X)^3,$$

which prove the lemma. □

Using this upper bound and the proof of [BKW00, Lemma 1], we have the following same result for $r_{ABij}(m)$ on minor arcs;

Proposition 3.4. *There is a positive real number $a = a(\delta)$ such that*

$$\sum_{\kappa N < n \le N} |r_{ABij}(2f(n); \mathfrak{m})| \ll XN^{1-\frac{a}{k}}. \tag{3.6}$$

Proof. We can observe that for all natural number l, $r_{ABij}(l, \mathfrak{m})$ is real. Define

$$\eta(l) = \begin{cases} 1 & \text{if } r_{ABij}(l, \mathfrak{m}) \ge 0, \\ -1 & \text{otherwise,} \end{cases} \qquad K(\alpha) = \sum_{\kappa N < n \le N} \eta(2f(n))e(2f(n)\alpha).$$

Then by the Hölder inequality,

$$\begin{aligned} \sum_{\kappa N < n \le N} |r_{ABij}(2f(n), \mathfrak{m})| &= \sum_{\kappa N < n \le N} \eta(2f(n)) r_{ABij}(2f(n), \mathfrak{m}) \\ &\le \int_{\mathfrak{m}} |S_i(A\alpha)S_j(B\alpha)K(-\alpha)|\, d\alpha \\ &\le \sup_{\alpha \in \mathfrak{m}} |S_i(A\alpha)S_j(B\alpha)|^{\frac{1}{t}} \Big(\int_{\mathfrak{m}} |S_i(A\alpha)S_j(B\alpha)| d\alpha \Big)^{1-\frac{1}{t}} \Big(\int_{\mathfrak{m}} |K(-\alpha)|^t d\alpha \Big)^{\frac{1}{t}} \end{aligned} \tag{3.7}$$

Since α is an element of minor arc, by Theorem 2.1 q is greater than P. Along with Lemma 3.3, we get

$$S_i(A\alpha) = \sum_{\substack{p \le X \\ p \equiv i}} \log p \cdot e(\alpha Ap) \ll (Xq^{-\frac{1}{2}} + X^{\frac{4}{5}} + X^{\frac{1}{2}}q^{\frac{1}{2}})(\log X)^3 \ll X^{1-3\delta}(\log X)^3.$$

This implies that the bound of the first multiplier of (3.7) is $[X^{1-3\delta}(\log X)^3]^2$. Now, let us analyze the second one. It can be calculated as

$$\int_{\mathfrak{m}} |S_i(A\alpha)S_j(B\alpha)|\, d\alpha \le \sum_{\substack{Ap+Bq=0 \\ p \equiv i, q \equiv j \\ P < p,q \le X}} \log p \log q \ll X \log X,$$

where the last inequality is followed by $\sum_{p\leq X}\log p \ll X$.
For the third multiplier, we can use the asymptotic of [BKW00, p.120] since the definition of $K(\alpha)$ does not change even if we use $S_i(A\alpha)$ instead of $S(\alpha)$. Therefore,

$$\int_0^1 |K(-\alpha)|^t d\alpha \ll N^{t-k(1-\delta)}.$$

By combining these results,

$$\sum_{\kappa N<n\leq N} |r_{ABij}(2f(n),\mathfrak{m})| \ll NX^{1-\frac{5\delta}{t}}(\log X)^2.$$

□

3.3 Major arc

We first introduce some classical facts about the zeros of Dirichlet L-functions. If χ is a primitive Dirichlet character of modulus $q \leq P$, then there exists $C > 0$ such that

$$L(s,\chi) \neq 0 \text{ for } s \geq 1 - \frac{C}{\log P}$$

with the only one possible exception $\tilde{\chi}$. If it exists, then we call it the *exceptional character*. Denote a modulus of exceptional character as $\tilde{r}$ and a zero of $L(s,\tilde{\chi})$ as $\tilde{\beta}$. This zero of L-function which is called *Siegel zero*, must be real and satisfy

$$\frac{C'}{\tilde{r}^{1/2}\log^2\tilde{r}} \leq 1-\tilde{\beta} \leq \frac{C}{\log P}.$$

(cf. [Dav, §. 14]). For a Dirichlet character χ, we define

$$\psi(x,\chi) = \sum_{n\leq x}\chi(n)\Lambda(n), \quad \psi(x,\chi,i) = \sum_{\substack{n\leq x \\ n\equiv i \pmod g}} \chi(n)\Lambda(n),$$

where $\Lambda(n)$ is the von Mangoldt function. As in the previous section, by the orthogonality relations of Dirichlet characters, we have

$$\psi(x,\chi,i) = \frac{1}{\varphi(g)}\sum_{n\leq x}\Big(\sum_{\chi'}\bar{\chi'}(i)\chi'(n)\Big)\chi(n)\Lambda(n) = \frac{1}{\varphi(g)}\sum_{\chi'}\bar{\chi'}(i)\psi(x,\chi\cdot\chi'),$$

where χ' varies in the set of Dirichlet characters of modulus g and $\chi \cdot \chi'(n) = \chi(n)\chi'(n)$. From the proof of [Gal70, Theorem 7], we have for $q \le T \le x^{\frac{1}{2}}$,

$$\psi(x,\chi,i) = \frac{1}{\varphi(g)} \sum_{\chi'} \bar{\chi}'(i)(\delta_{\chi\cdot\chi'} x - \sum_{\rho} \frac{x^\rho}{\rho}) + O(\frac{x \log^2 x}{T}),$$

and

$$\sum_{q\le P} \sideset{}{^*}\sum_{\chi} \sum_{\substack{x \\ p\equiv i \pmod g}}^{x+h} \chi(p)\log p \ll h(\sum_{q\le P} \sideset{}{^*}\sum_{\chi} \sum_{\chi'} \sum_{\rho} x^{\beta-1} + \frac{P^4}{T}),$$

where $\rho = \beta + \gamma i$ varies in the set of zeros of $L(s, \chi\cdot\chi')$ with $0 \le \mathrm{Re}(\rho) \le 1$, $|\mathrm{Im}(\rho)| \le T$ and $\sum^*$ denotes that the sum is taken over all primitive Dirichlet characters of modulus q. From the proof of [Gal70, Theorem 7], additional computations and the argument below [MV75, Lemma 4.3], we have the following modification of [MV75, Lemma 4.3], which was first proved in [AK87];

Proposition 3.5. *For suitable (small) positive absolute constants c_1, c_2,*

$$\sum_{q\le P} \sideset{}{^*}\sum_{\chi} \max_{x\le N} \max_{h\le N} (h + \frac{N}{P})^{-1} \Big| \sum_{\substack{x-h \\ p\equiv i \\ \pmod g}}^{x} {}^\sharp \chi(p)\log p \Big| \ll \exp(-c_1 \frac{\log N}{\log P}) \tag{3.8}$$

provided $\exp(\log^{\frac{1}{2}} N) \le P \le N^{c_2}$. *Here* $\sum^\sharp$ *indicates that the term with* $q = 1$ *is to be*

$$\sum_{\substack{x-h \\ p\equiv i \pmod g}}^{x} \log p - \sum_{\substack{x-h<n\le x \\ n>0 \\ n\equiv i \pmod g}} 1$$

and that if there is an exceptional character $\tilde{\chi}$ *then the corresponding term is*

$$\sum_{\substack{x-h \\ p\equiv i \pmod g}}^{x} \tilde{\chi}(p)\log p + \sum_{\substack{x-h<n\le x \\ n>0 \\ n\equiv i \pmod g}} n^{\tilde{\beta}-1},$$

where $\tilde{\beta}$ *is the (unique) exceptional zero of* $L(s,\tilde{\chi})$. *If the exceptional character occurs, the right hand side of (3.8) may be reduced by a factor of* $(1-\tilde{\beta})\log P$.

For a Dirichlet character χ of modulus q, we define

$$S_i(\chi,\eta)=\sum_{\substack{P<p\le X\\ p\equiv i \pmod g}}(\log p)\chi(p)e(p\eta),$$

and

$$T_i(\eta)=\sum_{\substack{P<n\le X\\ n\equiv i \pmod g}}e(n\eta),\qquad \widetilde{T}_i(\eta)=-\sum_{\substack{P<n\le X\\ n\equiv i \pmod g}}n^{\tilde{\beta}-1}e(n\eta),$$

where the last one is defined only if there is an exceptional character.
Let χ_0 be the principal character modulo q. Define

$$W_i(\chi,\eta)=\begin{cases} S_i(\chi,\eta)-T_i(\eta) & \text{if } \chi=\chi_0,\\ S_i(\chi,\eta)-\widetilde{T}_i(\eta) & \text{if } \chi=\tilde{\chi}\chi_0,\\ S_i(\chi,\eta) & \text{otherwise.}\end{cases}$$

Suppose that a Dirichlet character $\chi \pmod q$ is induced by a primitive character $\chi^* \pmod r$. Put

$$W_i^A(\chi)=\Big(\int_{-\frac{1}{rQ}}^{\frac{1}{rQ}}|W_i(\chi,A\eta)|^2\,d\eta\Big)^{\frac12},\qquad W_i^A=\sum_{q\le P}\sum_{\chi}{}^{*}W_i^A(\chi).$$

The following proposition is a modification of [MV75, (7.1) and (7.$\tilde{1}$)];

Proposition 3.6. *If there is no exceptional character,*

$$W_i^A\ll X^{\frac12}\exp(-c_3\frac{\log X}{\log P}),$$

and if the exceptional character occurs,

$$W_i^A\ll X^{\frac12}(1-\tilde{\beta})\log P\exp(-c_3\frac{\log X}{\log P}).$$

Proof. Applying [MV75, Lemma 4.2] to the real numbers

$$u_n = \begin{cases} \chi(p)\log p & \text{if } n = Ap,\ P < p \le X,\ p \equiv i \pmod g, \\ 0 & \text{otherwise,} \end{cases}$$

we get

$$\begin{aligned} W_i^A(\chi) &\ll \Big(\int_0^{2AX} \Big|\frac{1}{qQ} \sum_{\substack{P<p\le X \\ x-\frac{qQ}{2}\le Ap\le x \\ p\equiv i \pmod g}} {}^\sharp\chi(p)\log p\Big|^2 dx\Big)^{\frac12} \\ &\ll X^{\frac12} \max_{x\le 2X}\max_{0<h\le X}(h+\frac{X}{P})^{-1}\Big|\sum_{\substack{x-h \\ p\equiv i \\ (\mathrm{mod}\, g)}}^{x} {}^\sharp\chi(p)\log p\Big|. \end{aligned}$$

Then using the above modification of [MV75, Lemma 4.3], we have the proposition. □

For $\alpha \in \mathfrak{M}(q,a)$ we write $\alpha = \frac{a}{q} + \eta$ for $(a,q) = 1$, $-\frac{1}{qQ} \le \eta < \frac{1}{qQ}$ and $q < P$. For a character χ of modulus q, let $\tau(\chi) = \sum_{n=1}^{q} \chi(n) e(\frac{n}{q})$ be the Gaussian sum. For integers $C, D \in \{A, B, q, n, 2f(n)\}$, we define $C_D = \frac{C}{(C,D)}$. Using arguments in [MV75, Section 6], we have

$$S_i(A\alpha) = \frac{\mu(q_A)}{\varphi(q_A)} T_i(A\eta) + \frac{1}{\varphi(q_A)} \sum_{\chi} \chi(A_q a)\tau(\bar\chi) W_i(\chi, A\eta), \tag{3.9}$$

where the sum is over all Dirichlet characters χ of modulus q_A, unless there is an exceptional character of modulus $\tilde r$, in which case $\tilde r | q_A$ then we obtain an additional term

$$\frac{\tilde\chi(A_q a)\tau(\tilde\chi\chi_0)}{\varphi(q_A)} \widetilde{T}_i(A\eta)$$

on the right hand side of (3.9).

Proposition 3.7. *Suppose that Y is a real number with $1 \le Y \le X^{\frac{\delta}{k}}$. Then one has*

$$r_{ABij}(2f(n); \mathfrak{M}) \gg XY^{-\frac12}(\log X)^{-1} \tag{3.10}$$

for all $n \in (\kappa N, N]$ *with* $2f(n) \equiv Ai + Bj \pmod 9$ *and* $(AB, 2f(n)) = 1$ *with the possible exception of* $O(N^{1+\epsilon}Y^{-1})$ *values of* n.

Proof. First we assume that there is no exceptional character. Let $n \in (\kappa N, N]$ be an integer with $2f(n) \equiv Ai + Bj \pmod 9$ and $(AB, 2f(n)) = 1$. For simplicity, we define

$$\begin{aligned} t_i^A t_j^B(\eta) &= T_i(A\eta)T_j(B\eta)e(-2f(n)\eta), \\ t_i^A w_j^B(\eta) &= T_i(A\eta)W_j(\chi', B\eta)e(-2f(n)\eta), \\ t_j^B w_i^A(\eta) &= T_j(B\eta)W_i(\chi, A\eta)e(-2f(n)\eta), \\ w_i^A w_j^B(\eta) &= W_i(\chi, A\eta)W_j(\chi', B\eta)e(-2f(n)\eta), \end{aligned}$$

where χ and χ' are characters of modulus of q_A and q_B, respectively. Then we have

$$\begin{aligned} & r_{ABij}(2f(n); \mathfrak{M}) \\ = & \sum_{q \le P} \frac{\mu(q_A)\mu(q_B)}{\varphi(q_A)\varphi(q_B)} c_q(-2f(n)) \int_{-\frac{1}{qQ}}^{\frac{1}{qQ}} t_i^A t_j^B(\eta) d\eta & (3.11) \\ + & \sum_{q \le P} \frac{\mu(q_A)}{\varphi(q_A)\varphi(q_B)} \sum_{\chi'} \chi'(B_q) c_{\chi'}(-2f(n)) \tau(\bar{\chi'}) \int_{-\frac{1}{qQ}}^{\frac{1}{qQ}} t_i^A w_j^B(\eta) d\eta & (3.12) \\ + & \sum_{q \le P} \frac{\mu(q_B)}{\varphi(q_A)\varphi(q_B)} \sum_{\chi} \chi(A_q) c_{\chi}(-2f(n)) \tau(\bar{\chi}) \int_{-\frac{1}{qQ}}^{\frac{1}{qQ}} t_j^B w_i^A(\eta) d\eta & (3.13) \\ + & \sum_{q \le P} \frac{1}{\varphi(q_A)\varphi(q_B)} (\sum_{\chi, \chi'} \chi(A_q)\chi'(B_q) c_{\chi\chi'}(-2f(n)) \tau(\bar{\chi})\tau(\bar{\chi'}) \\ \times & \int_{-\frac{1}{qQ}}^{\frac{1}{qQ}} w_i^A w_j^B(\eta) d\eta), & (3.14) \end{aligned}$$

where $c_q(m) = \sum_{(a,q)=1}^{q} e(\frac{am}{q})$ and $c_*(m) = \sum_{h=1}^{q} *(h) e(\frac{hm}{q})$ (We remark that h goes from 1 to q though the modulus of $*$ is a divisor of q.).

Using [MV75, Lemma 5.5] and arguments in [MV75, Section 6], we have

$$\begin{aligned}(3.12) &\ll X^{\frac{1}{2}} \sum_{q\le P} \sum_{\chi'} |\frac{\mu(q_A)\chi'(B_q)c_{\chi'}(-2f(n))\tau(\bar{\chi'})}{\varphi(q_A)\varphi(q_B)}|(\int_{-\frac{1}{rQ}}^{\frac{1}{rQ}} \left|W_j(\chi', B\eta)\right|^2 d\eta)^{\frac{1}{2}} \\ &\ll X^{\frac{1}{2}} \sum_{q\le P} \sum_{\chi'} |\frac{c_{\chi'}(-2f(n))\tau(\bar{\chi'})}{\varphi(q)^2}|(\int_{-\frac{1}{rQ}}^{\frac{1}{rQ}} \left|W_j(\chi', B\eta)\right|^2 d\eta)^{\frac{1}{2}} \\ &\ll \frac{2f(n)}{\varphi(2f(n))} W_j^B X^{\frac{1}{2}}.\end{aligned}$$

By the same method, we have

$$(3.13) \ll \frac{2f(n)}{\varphi(2f(n))} W_i^A X^{\frac{1}{2}} \quad \text{and} \quad (3.14) \ll \frac{2f(n)}{\varphi(2f(n))} W_i^A W_j^B.$$

Now we consider the term (3.11). Assume harmless conditions $qQ > 2gA$ and $A \ge B$. Then we have

$$\begin{aligned}\int_{-\frac{1}{qQ}}^{\frac{1}{qQ}} t_i^A t_j^B(\eta)d\eta &= \int_{-\frac{1}{2g}}^{\frac{1}{2g}} t_i^A t_j^B(\eta)d\eta - \int_{\frac{1}{2gA}}^{\frac{1}{2g}} t_i^A t_j^B(\eta)d\eta - \int_{-\frac{1}{2g}}^{-\frac{1}{2gA}} t_i^A t_j^B(\eta)d\eta \\ &\quad - \int_{\frac{1}{qQ}}^{\frac{1}{2gA}} t_i^A t_j^B(\eta)d\eta - \int_{-\frac{1}{2gA}}^{-\frac{1}{qQ}} t_i^A t_j^B(\eta)d\eta.\end{aligned}$$

By the same argument for [MV75, (6.10)], we have

$$\int_{\frac{1}{qQ}}^{\frac{1}{2gA}} t_i^A t_j^B(\eta)d\eta \ll \int_{\frac{1}{qQ}}^{\frac{1}{2gA}} \frac{1}{\|gA\eta\|}\frac{1}{\|gB\eta\|}d\eta \le \int_{\frac{1}{qQ}}^{\frac{1}{2gA}} \frac{1}{g^2AB\eta^2}d\eta \ll qQ.$$

where $\|a\|$ is defined by $\min_{x\in\mathbb{Z}} |a-x|$. Also,

$$\int_{-\frac{1}{2g}}^{\frac{1}{2g}} t_i^A t_j^B(\eta)d\eta = \sum_{\substack{P<k,l\le X \\ k\equiv i, l\equiv j \\ Ak+Bl=2f(n)}} \frac{1}{g} = \frac{2f(n)}{g^3AB} + O(P)$$

and

$$\begin{aligned}\int_{\frac{1}{2gA}}^{\frac{1}{2g}} t_i^A t_j^B(\eta)d\eta &= \sum_{\substack{P<k,l\le X\\ k\equiv i, l\equiv j\\ Ak+Bl=2f(n)}} (\frac{1}{2g}-\frac{1}{2gA})+O(\log X)\\ &= (\frac{1}{2g}-\frac{1}{2gA})\frac{2f(n)}{g^2AB}+O(P).\end{aligned}$$

Thus we have

$$\int_{-\frac{1}{qQ}}^{\frac{1}{qQ}} t_i^A t_j^B(\eta)d\eta = \frac{2f(n)}{g^3AB}-2(\frac{1}{2g}-\frac{1}{2gA})\frac{2f(n)}{g^2AB}+O(qQ).$$

Using the above estimations for the integral in (3.11) and arguments for [MV75, (6.12), (6.13), (6.14)], we have the the following estimation for the term (3.11);

$$(3.11) = \mathfrak{S}_{A,B}(2f(n))\frac{2f(n)}{g^3A^2B}+O(X^{1+\delta}P^{-1}),$$

where $\mathfrak{S}_{A,B}(n)=\sum_{q=1}^{\infty}\frac{\mu(q_A)\mu(q_B)}{\varphi(q_A)\varphi(q_B)}c_q(-n)$.

Finally, combining the above bounds for (3.12), (3.13), (3.14) and the above estimation for (3.11), we have the following modification of [MV75, (6.17)];

$$\begin{aligned}r_{ABij}(2f(n);\mathfrak{M}) &= \mathfrak{S}_{A,B}(2f(n))\frac{2f(n)}{g^3A^2B}+O(X^{1+\delta}P^{-1})\\ &+ O(\frac{2f(n)}{\varphi(2f(n))}(W_i^AX^{\frac{1}{2}}+W_j^BX^{\frac{1}{2}}+W_i^AW_j^B)). \quad (3.15)\end{aligned}$$

Since A, B and $2f(n)$ are pairwise relatively prime, we have

$$\begin{aligned}\mathfrak{S}_{A,B}(2f(n)) &= \prod_p(1+\frac{\mu(p_A)\mu(p_B)\mu(p_{(2f(n))})\varphi(p)}{\varphi(p_A)\varphi(p_B)\varphi(p_{(2f(n))})})\\ &= \prod_{p|(2f(n))AB}(1+\frac{1}{\varphi(p)})\prod_{p\nmid(2f(n))AB}(1-\frac{1}{\varphi(p)^2})\end{aligned}$$

and by [BKW00, (15)]

$$\mathfrak{S}_{A,B}(2f(n)) = c_{A,B}\mathfrak{S}_{1,1}(2f(n)) \ge c_{A,B}\frac{2f(n)}{\varphi(2f(n))}$$

for a constant $c_{A,B}$ depending only on A, B. From the above modification of [MV75, (7.1)], the third term of the right hand side of (3.15) is less then $\frac{6f(n)}{\varphi(2f(n))}Xe^{-\frac{c_3}{6\delta}}$. If we choose a sufficiently small positive real number δ, then $r_{ABij}(2f(n);\mathfrak{M}) \geq (\frac{c_{A,B}}{9^3A^2B} - c_4)\mathfrak{S}(2f(n))(2f(n))$. This implies that

$$r_{ABij}(2f(n);\mathfrak{M}) \gg X.$$

Next we assume that there is the exceptional character. Let $n \in (\kappa N, N]$ be an integer with $2f(n) \equiv Ai + Bj \pmod{g}$ and $(AB, 2f(n)) = 1$. For simplicity, we define

$$\begin{aligned}
\widetilde{t}_i^A\widetilde{t}_j^B(\eta) &= \widetilde{T}_i(A\eta)\widetilde{T}_j(B\eta)e(-2f(n)\eta),\\
t_i^A\widetilde{t}_j^B(\eta) &= T_i(A\eta)\widetilde{T}_j(B\eta)e(-2f(n)\eta),\\
\widetilde{t}_i^A t_j^B(\eta) &= \widetilde{T}_i(A\eta)T_j(B\eta)e(-2f(n)\eta),\\
\widetilde{t}_i^A w_j^B(\eta) &= \widetilde{T}_i(A\eta)W_j(\chi', B\eta)e(-2f(n)\eta),\\
\widetilde{t}_j^B w_i^A(\eta) &= \widetilde{T}_j(B\eta)W_i(\chi, A\eta)e(-2f(n)\eta),
\end{aligned}$$

where χ and χ' are characters of modulus of q_A and q_B, respectively. Then we have the following possible additional terms in $r_{ABij}(2f(n);\mathfrak{M})$;

$$\sum_{\substack{q\leq P\\ \tilde{r}|q_A,q_B}} \frac{\tau(\tilde{\chi}\chi_0)\tau(\tilde{\chi}\chi_0')}{\varphi(q_A)\varphi(q_B)}\tilde{\chi}(A_qB_q)c_q(-2f(n))\int_{-\frac{1}{qQ}}^{\frac{1}{qQ}} \widetilde{t}_i^A\widetilde{t}_j^B(\eta)d\eta \tag{3.16}$$

$$+ \sum_{\substack{q\leq P\\ \tilde{r}|q_B}} \frac{\mu(q_A)\tau(\tilde{\chi}\chi_0')}{\varphi(q_A)\varphi(q_B)}\tilde{\chi}(B_q)c_{\tilde{\chi}\chi_0'}(-2f(n))\int_{-\frac{1}{qQ}}^{\frac{1}{qQ}} t_i^A\widetilde{t}_j^B(\eta)d\eta \tag{3.17}$$

$$+ \sum_{\substack{q\leq P\\ \tilde{r}|q_A}} \frac{\mu(q_B)\tau(\tilde{\chi}\chi_0)}{\varphi(q_A)\varphi(q_B)}\tilde{\chi}(A_q)c_{\tilde{\chi}\chi_0}(-2f(n))\int_{-\frac{1}{qQ}}^{\frac{1}{qQ}} \widetilde{t}_i^A t_j^B(\eta)d\eta \tag{3.18}$$

$$+ \sum_{\substack{q\leq P\\ \tilde{r}|q_B}} \frac{\tilde{\chi}(B_q)\tau(\tilde{\chi}\chi_0')}{\varphi(q_A)\varphi(q_B)}\Big(\sum_{\chi} c_{\tilde{\chi}\chi}(-2f(n))\tau(\bar{\chi})\chi(A_q)\int_{-\frac{1}{qQ}}^{\frac{1}{qQ}} \widetilde{t}_j^B w_i^A(\eta)d\eta\Big) \tag{3.19}$$

$$+ \sum_{\substack{q\leq P\\ \tilde{r}|q_A}} \frac{\tilde{\chi}(A_q)\tau(\tilde{\chi}\chi_0)}{\varphi(q_A)\varphi(q_B)}\Big(\sum_{\chi'} c_{\tilde{\chi}\chi'}(-2f(n))\tau(\bar{\chi'})\chi'(B_q)\int_{-\frac{1}{qQ}}^{\frac{1}{qQ}} \widetilde{t}_i^A w_j^B(\eta)d\eta\Big). \tag{3.20}$$

By the same arguments for (3.12) and (3.13), we have

$$(3.19) \ll \frac{2f(n)}{\varphi(2f(n))} W_i^A X^{\frac{1}{2}} \quad \text{and} \quad (3.20) \ll \frac{2f(n)}{\varphi(2f(n))} W_j^B X^{\frac{1}{2}}.$$

Now we consider the first three terms (3.16), (3.17), (3.18). For the integral in (3.16), we have

$$\int_{\frac{1}{2gA}}^{\frac{1}{2g}} \widetilde{t}_i^A \widetilde{t}_j^B(\eta) d\eta = \sum_{\substack{P<k,l\leq X \\ k\equiv i, l\equiv j \\ Ak+Bl=2f(n)}} (kl)^{\tilde{\beta}-1}(\frac{1}{2g} - \frac{1}{2gA}) + O(\log X)$$

and by the same argument for the estimation of the integral in (3.11), we have

$$\int_{-\frac{1}{qQ}}^{\frac{1}{qQ}} \widetilde{t}_i^A \widetilde{t}_j^B(\eta) d\eta = \widetilde{I}_{ij}^{AB} - 2 \sum_{\substack{P<k,l\leq X \\ k\equiv i, l\equiv j \\ Ak+Bl=2f(n)}} (kl)^{\tilde{\beta}-1}(\frac{1}{2g} - \frac{1}{2gA}) + O(qQ),$$

where

$$\widetilde{I}_{ij}^{AB} = \int_{-\frac{1}{2g}}^{\frac{1}{2g}} \widetilde{t}_i^A \widetilde{t}_j^B(\eta) d\eta = \sum_{\substack{P<k,l\leq X \\ k\equiv i, l\equiv j \\ Ak+Bl=2f(n)}} (kl)^{\tilde{\beta}-1}(\frac{1}{g}).$$

Similarly, for the integral in (3.17), we have

$$\int_{-\frac{1}{qQ}}^{\frac{1}{qQ}} t_i^A \widetilde{t}_j^B(\eta) d\eta = \widetilde{J}_{ij}^{AB} - 2 \sum_{\substack{P<k,l\leq X \\ k\equiv i, l\equiv j \\ Ak+Bl=2f(n)}} (l)^{\tilde{\beta}-1}(\frac{1}{2g} - \frac{1}{2gA}) + O(qQ),$$

where $\widetilde{J}_{ij}^{AB} = \int_{-\frac{1}{2g}}^{\frac{1}{2g}} t_i^A \widetilde{t}_j^B(\eta) d\eta$ and for the integral in (3.18), we have

$$\int_{-\frac{1}{qQ}}^{\frac{1}{qQ}} \widetilde{t}_i^A t_j^B(\eta) d\eta = \widetilde{J}_{ji}^{BA} - 2 \sum_{\substack{P<k,l\leq X \\ k\equiv i, l\equiv j \\ Ak+Bl=2f(n)}} (k)^{\tilde{\beta}-1}(\frac{1}{2g} - \frac{1}{2gA}) + O(qQ),$$

where $\widetilde{J}_{ji}^{BA} = \int_{-\frac{1}{2g}}^{\frac{1}{2g}} \widetilde{t}_i^A t_j^B(\eta) d\eta$.

Using the arguments for [MV, (6.19), (6.16)], we have

$$\begin{aligned}(3.16)+(3.17)+(3.18) &= \widetilde{\mathfrak{S}}_{A,B}(2f(n))\frac{\widetilde{I}_{ij}^{AB}}{A} \\ &+ O(\frac{\tilde{\chi}(2f(n))^2\tilde{r}\cdot 2f(n)X}{\varphi(\tilde{r})^2\varphi(2f(n))}) + O(X^{1+\delta}P^{-1}(2f(n),\tilde{r})),\end{aligned}$$

where $\widetilde{\mathfrak{S}}_{A,B}(n) = \sum_{\substack{q=1 \\ \tilde{r}|q_A,q_B}}^{\infty} \frac{\tau(\tilde{\chi}\chi_0)\tau(\tilde{\chi}\chi_0')}{\varphi(q_A)\varphi(q_B)}\widetilde{\chi}(A_qB_q)c_q(-n)$. Since A, B and $2f(n)$ are pairwise relatively prime and one of the Gaussian sums in $\widetilde{\mathfrak{S}}_{A,B}(n)$ vanishes when $q/\tilde{r}$ and $\tilde{r}$ are not relatively prime, we have

$$\widetilde{\mathfrak{S}}_{A,B}(2f(n)) = \frac{\tilde{\chi}(-AB)\tilde{r}}{\varphi(\tilde{r})\varphi(\tilde{r}_{2f(n)})} \prod_{\substack{p\nmid\tilde{r} \\ p|(2f(n))AB}} (1+\frac{1}{\varphi(p)}) \prod_{\substack{p\nmid\tilde{r} \\ p\nmid(2f(n))AB}} (1-\frac{1}{\varphi(p)^2}).$$

Finally, combining all the above estimations, we have the following modification of [MV75, (6.17)];

$$\begin{aligned}r_{ABij}(2f(n);\mathfrak{M}) &= \mathfrak{S}_{A,B}(2f(n))\frac{2f(n)}{g^3A^2B} + \widetilde{\mathfrak{S}}_{A,B}(2f(n))\frac{\widetilde{I}_{ij}^{AB}}{A} \\ &+ O(\frac{\tilde{\chi}(2f(n))^2\tilde{r}\cdot 2f(n)X}{\varphi(\tilde{r})^2\varphi(2f(n))}) + O(X^{1+\delta}P^{-1}(2f(n),\tilde{r})) \\ &+ O(\frac{2f(n)}{\varphi(2f(n))}(W_i^A X^{\frac{1}{2}} + W_j^B X^{\frac{1}{2}} + W_i^A W_j^B)). \qquad (3.21)\end{aligned}$$

If $(2f(n),\tilde{r}) = 1$, the fourth term of the right hand side of (3.21) is less then $X^{1-5\delta}$ and

$$\widetilde{\mathfrak{S}}_{A,B}(2f(n)) \ll \frac{\tilde{r}}{\varphi(\tilde{r})^2} \prod_{\substack{p\nmid\tilde{r} \\ p|2f(n)}} (1+\frac{1}{\varphi(p)}) \ll \frac{\tilde{r}\cdot 2f(n)}{\varphi(\tilde{r})^2\varphi(2f(n))} = o(1),$$

so using arguments in [MV75, Section 8] and the above modification of [MV75, (7.$\tilde{1}$)], we have $r_{ABij}(2f(n);\mathfrak{M}) \gg X$. Since

$$|\widetilde{\mathfrak{S}}_{A,B}(2f(n))| \;\leq\; \mathfrak{S}_{A,B}(2f(n)) \prod_{\substack{p|\tilde{r}\\ p\nmid(2f(n))AB}} \frac{1}{(p-2)} \prod_{\substack{p|\tilde{r}\\ p\nmid 2f(n)\\ p|AB}} \frac{1}{(p-1)}, \quad (3.22)$$

using arguments in [BKW00, p.122–123], we have that if $1 < (2f(n), \tilde{r}) \leq Y$,

$$r_{ABij}(2f(n);\mathfrak{M}) \gg \begin{cases} X & \text{if } \mathcal{P} \neq \varnothing, \\ XY^{-\frac{1}{2}}(\log X)^{-1} & \text{if } \mathcal{P} = \varnothing, \end{cases}$$

where $\mathcal{P}$ is the set of primes in the products of (3.22). Finally there are at most $O(N^{1+\epsilon}Y^{-1})$ possible exceptions n with $(2f(n), \tilde{r}) > Y$. □

Proof of Theorem 3.2. It is follows from Proposition 3.6, Proposition 3.7 and the proof of [BKW00, Theorem 1]. In general, if $\sum_{k=1}^{N} a_k \ll A$, then $a_k \ll \frac{A}{N}$ with possible $E_1 \ll \dfrac{N}{A}\sum_{k=1}^{N} a_k$ exceptions. By Proposition 3.6

$$\sum_{\kappa N < n \leq N} |r_{ij}^{AB}(2f(n), \mathfrak{m})| \ll XN^{1-\frac{a}{k}},$$

we get $r(2f(n);\mathfrak{m}) \ll XY^{-1}$ with at most E_1 possible exceptions where $Y = N^{\tau/k}$ for $\tau = \frac{1}{2}\min(a, \delta)$ and

$$E_1 \ll \frac{Y}{X} \sum_{\kappa N < n \leq N} |r_{ij}^{AB}(2f(n), \mathfrak{m})| \ll NY^{-1}.$$

By the way Proposition 3.7 tells us $r(2f(n), \mathfrak{M}) \gg XY^{-\frac{1}{2}}(\log X)^{-1}$ with at most $O(N^{1+\epsilon}Y^{-1})$ exceptions. Therefore

$$r(2f(n)) = r(2f(n), \mathfrak{m}) + r(2f(n), \mathfrak{M}) > 0$$

with at most $O(N^{1-\tau/k+\epsilon})$ exceptions. □

We note that if there is at least one integer m such that $2f(m) \equiv Ai + Bj \pmod{g}$ and $(AB, 2f(m)) = 1$, the set of $n \in (\kappa N, N]$ with $2f(n) \equiv Ai + Bj \pmod{g}$ and $(AB, 2f(n)) = 1$ has a positive density in the set of $n \in (\kappa N, N]$.

Chapter 4

Sum of two rational cubes

4.1 Previous results and Main theorem

We start with a classical question: which integers can be represented by a sum of two rational cubes? In the view of Diophantine equations, this question exactly asks that for which integer n there is a rational point in the projective curve

$$x^3 + y^3 = nz^3.$$

One can easily notice that this curve has a structure of the elliptic curves, and its Weierstrass equation is

$$y^2 = x^3 - 432n^2.$$

In this chapter, we denote this elliptic curve by E_n. We will show that the root number w_n of the elliptic curve E_n is -1 if n is equivalent to 4, 6, 7, or 8 modulo 9. (Lemma 4.5) Hence under the parity conjecture, such integers can be represented by a sum of two rational cubes.

There are some results which show that for some $n \equiv 4, 7, 8 \pmod 9$ are sums of two rational cubes without assuming the parity conjecture. In [Sat87], Satgé proved that $n = 2p$, where p is a prime congruent to 2 modulo 9, and also

$n = 2p^2$, where p is a prime congruent to 5 modulo 9, are sums of two rational cubes. Coward [Cow00] proved that $n = 25p$, where p is a prime congruent to 2 modulo 9, and also $n = 25p^2$, where p is a prime congruent to 5 modulo 9, are sums of two rational cubes. In [DV09], Dasgupta and Voight proved that if p is a prime congruent to 4 or 7 modulo 9 and 3 is not a cube mod p, then p is a sum of two rational cubes.

Note in all cases the root number of corresponding elliptic curves is -1, and the number of the prime factor of n is less than 2. We will show that there are infinitely many integers n which is a sum of two rational cubes, has arbitrary large number of prime divisors, and has arbitrary root number.

Theorem 4.1. *For any given integer $k \geq 2$ and $e \in \{1, -1\}$, there are infinitely many cube-free integers (in fact, square-free integers) n having exactly k prime divisors such that n is a sum of two rational cubes and $w_n = e$.*

In [Tia14], Tian has shown that for any given integer $k \geq 1$, there are infinitely many square-free positive integers m such that m is a congruent number and the corresponding elliptic curve $E : y^2 = x^3 - m^2x$ has the root number -1. So Theorem 4.1 for the case $w_n = -1$ is a cubic analogue of the work of Tian.

On the other hand, Coates and Wiles [CW77] proved that if n is a sum of two rational cubes, than the analytic rank of E_n is greater than zero. So we immediately have the following corollary from Theorem 4.1 for the case $w_n = 1$.

Corollary 4.2. *For any given integer $k \geq 2$, there are infinitely many cube-free integers n having exactly k prime divisors such that the analytic rank of E_n is at least 2.*

4.2 Some properties of E_n

In this section, we will prove some properties of the elliptic curve E_n, given by an equation $x^3 + y^3 = nz^3$ or a Weierstrass equation $y^2 = x^3 - 432n^2$. We assume that n is a cube-free integer, since the elliptic curve E_{nm^3} is isomorphic to E_n as a $G_{\mathbb{Q}}$-module.

Lemma 4.3. *When n is a cube-free integer, the torsion subgroup of Mordell–Weil group of $E_n(\mathbb{Q})$ is trivial if $n \neq \pm 1$ and $n \neq \pm 2$, and $\mathbb{Z}/3\mathbb{Z}$ if $n = \pm 1$ or $n = \pm 2$.*

Proof. By Nagell-Lutz theorem. [Sil09, Exercises 10.19]. □

In [Mai93, Lemma 2.1], Mai proves the following lemma.

Lemma 4.4. *E_n has integral points if and only if n has one of the following six forms:*

$$n = \pm\frac{b(a^2 - b^2)}{4} \text{ or } n = \pm\frac{3a^2b - 3b^3}{24} \pm \frac{a^3 - 9ab^2}{24} \text{ for some } a, b \in \mathbb{Z}.$$

Proof. Let (X, Y) be an integral point of a Weierstrass equation of $E_n : y^2 = x^3 - 432n^2$. Then, there is a factorization of ideals in a Dedekind domain $O_{\mathbb{Q}(\sqrt{-3})}$,

$$(X)^3 = (Y + 12n\sqrt{-3})(Y - 12n\sqrt{-3}).$$

When an ideal $\mathfrak{p}$ of $O_{\mathbb{Q}(\sqrt{-3})}$ divides $(Y + 12m\sqrt{-3})$, then $\overline{\mathfrak{p}}$ divides $(Y - 12n\sqrt{-3})$. Therefore,

$$(X)^3 = \prod \mathfrak{p}_i^{m_i}\overline{\mathfrak{p}_i}^{m_i} = \prod p_i^{a_i m_i}.$$

Since a_i divides 2, m_i is divided by 3 for all i. The ideal $(Y + 12n\sqrt{-3})$ is principal, so

$$Y + 12n\sqrt{-3} = u(a + b\sqrt{-3})^3$$

for $a, b \in \mathbb{Z}$ and $u \in O^{\times}_{\mathbb{Q}(\sqrt{-3})} = \left\{\pm 1, \pm\frac{1}{2} \pm \frac{\sqrt{3}}{2}\right\}$. In each case,

$$n = \pm\frac{b(a^2-b^2)}{4} \text{ or } n = \pm\frac{3a^2b-3b^3}{24} \pm \frac{a^3-9ab^2}{24}.$$

Conversely, when n is one of above form, there is an integral point on E_n, namely

$$(X,Y) = (a^2+3b^2, \pm(a^3-9ab^2)), \text{ or } (a^2+3b^2, \pm\frac{1}{2}(a^3-9ab^2) \pm \frac{-3}{2}(3a^2b-3b^3)).$$

□

Lemma 4.5. *Let $n > 0$ be a square-free integer. Then*

$$w_n = \begin{cases} +1 & \text{if } n \equiv 1, 2, 3 \text{ or } 5 \pmod 9 \\ -1 & \text{if } n \equiv 4, 6, 7 \text{ or } 8 \pmod 9. \end{cases}$$

Proof. Write the prime factorization of n in the form

$$n = 3^{\alpha} \prod_{p_i \equiv 1 \pmod 3} p_i \prod_{q_j \equiv 2 \pmod 3} q_j,$$

where $\alpha = 0$ or 1 and p_i, q_j are distinct primes. Let a_n be the number of $q_j \equiv 2 \pmod 3$. Then the computation of local root number $w_n(p)$ of E_n in [BS66] gives the following condition: for the prime number $p \neq 3$,

$$w_n(p) = \begin{cases} -1 & \text{if } p \mid n, \text{ and } p \equiv 2 \pmod 3, \\ +1 & \text{otherwise,} \end{cases}$$

and for $p = 3$,

$$w_n(3) = \begin{cases} +1 & \text{if } n \equiv \pm 1, \pm 3 \pmod 9 \\ -1 & \text{otherwise.} \end{cases}$$

We note that $n/3^{\alpha} \equiv 2 \pmod 3$ if and only if a_n is odd. Then by

$$w_n = \prod_p w_n(p),$$

we can prove this lemma. For example when $n \equiv 1 \pmod 9$, a_n is even and $w_n(3) = +1$ which shows that $w_n = 1$ if $n \equiv 1 \pmod 9$. The other cases can be proved in the same way. □

4.3 Proof of the first application

The following proposition is a main tool to prove Theorem 4.1.

Proposition 4.6. *For any given $k \geq 2$ and $r \in \{1, 2, 4, 5, 7, 8\}$, there are infinitely many square-free integers $n > 0$ having exactly k prime divisors such that n is a sum of two rational cubes and $n \equiv r \pmod 9$. For $r \in \{3, 6\}$, the same statement holds for $k \geq 3$.*

Proof. By Lemma 4.4, we know that for nonzero $a, b \in \mathbb{Z}$, $16b^6 - a^2$ is a sum of two rational cubes because $b^3(16b^6 - a^2) = -\frac{(4b^3)(a^2-(4b^3)^2)}{4}$. Let

$$A = \prod_{i=1}^{l} p_i, \text{ for fixed primes } p_i \equiv 1 \pmod 9, \ B = 27,$$

where $l \geq 0$ is a fixed integer (if $l = 0$, then $A = 1$).

We note that $b^3 \equiv 0$ or $\pm 1 \pmod 9$ for any integer b. Since there is an integer b such that $8b^3 \equiv 8A + 8B \pmod 9$ and $(AB, 8b^3) = 1$, Theorem 3.2 ensures that there are infinitely many integers b that satisfy the equation

$$4b^3 = \frac{Ap + Bq}{2},$$

for some primes $p \equiv 8$ and $q \equiv 8 \pmod 9$. If $p = q$, then $8b^3 = Ap + 27p$, so $8p^2c^3 = A + 27$ for some positive integer c. Thus there are only finitely many p, q such that $p = q$ and we may assume $p \neq q$.

Let $a = \frac{Ap-Bq}{2} \in \mathbb{Z}$. Then $16b^6 - a^2 = ABpq = 27Apq$ is a sum of two rational cubes having exactly $(l + 3)$ prime divisors because $p, q \nmid A, B$. Hence Apq is a square-free integer having exactly $(l+2)$ prime divisors such that Apq is sum of two rational cubes and $Apq \equiv 1 \pmod 9$. This proves the theorem for the case of $r = 1$. If we set $q \equiv 7, 5, 4$ and $2 \pmod 9$, then the theorem for the cases of $r = 2$, 4, 5, and 7 follows.

For the case $r = 8$ and $k \geq 3$, set

$$A = \prod_{i=1}^{l} p_i, \quad \text{for fixed primes } p_1 \equiv 2, \ p_2, \cdots, p_l \equiv 1 \pmod 9, \ B = 27$$

and let p, q be primes such that $p \equiv 5,\ q \equiv 8 \,(\mathrm{mod}\ 9)$. For the case $r = 8$ and $k = 2$, set

$$A = 1,\ B = 27$$

and let p, q be primes such that $p \equiv 8,\ q \equiv 1 \ (\mathrm{mod}\ 9)$. Then the theorem for the case $r = 8$ follows.

For the case $r = 3$, let

$$A = \prod_{i=1}^{l} p_i, \ \text{ for fixed primes } p_i \equiv 1 \ (\mathrm{mod}\ 9),\ B = 81,$$

where $l \geq 0$ is a fixed integer (if $l = 0$, then $A = 1$) and let p, q be primes such that $p \equiv 8$, $q \equiv 8 \ (\mathrm{mod}\ 9)$ Then $3Apq$ is a square-free integer having exactly $(l+3)$ prime divisors such that $3Apq$ is sum of two rational cubes and $3Apq \equiv 3 \ (\mathrm{mod}\ 9)$. This proves the theorem for the case of $r = 3$. Finally, if we set $q \equiv 7 \ (\mathrm{mod}\ 9)$, then the theorem for the case $r = 6$ follows and the proof of the theorem is completed. □

Proof of Theorem 4.1. Lemma 4.5 and Proposition 4.6 for the case $r = 4, 7, 8$ implies Theorem 4.1 for the case $w_n = -1$. Lemma 4.5 and Proposition 4.6 for the case $r = 1, 2, 5$ implies Theorem 4.1 for the case $w_n = 1$.

Chapter 5

Ranks of family of elliptic curves

5.1 Mordell–Weil group of a family of elliptic curves

For a small positive integer r, there are various results on the existence of elliptic curves of rank greater than r, using specialization theorem of Néron [Ner52]. (cf. [SS], and for concrete examples, [Mes98]) The highest record of rank of the elliptic curve over $\mathbb{Q}$ is ≥ 28, due to Elkies. It means that there is an elliptic curve over $\mathbb{Q}$ which has 28 independent points. The torsion subgroup of this elliptic curves is trivial, so the natural question arise : which number n can be a rank of elliptic curve with prescribed torsion subgroup? The current records for this problem can be found in [Duj1]. We have to remark that in general when the torsion group is larger, then the rank record will be small. As we remarked when the torsion is trivial the record is 28, but when the torsion subgroup is $\mathbb{Z}/12\mathbb{Z}$, the record is only 4 [Duj2].

There are also numerous results which construct an infinite family of elliptic curves whose rank is at least r. The current record is ≥ 18 whose torsion groups are all trivial, also due to Elkies. When the size of prescribed torsion subgroups is larger, the rank records of a family of elliptic curves also decrease.

For example, when the torsion subgroups are $\mathbb{Z}/12\mathbb{Z}$, the record is just 0. Note that [Duj3] also introduces the current records for these problems.

On the other hand, some are interested in finding an elliptic curve with *exact* rank r. The highest record, also due to Elkies, is 19. Bober [Bob11] shows that there is an elliptic curve with rank 20, 21, 22, 23, 24 under the generalized Riemann Hypothesis and Birch–Swinnerton-Dyer conjecture, and in [KSW16] the authors showed that there is an elliptic curve with rank 27, and 28 under the generalized Riemann Hypothesis.

However less is known for the existence of an *infinite family* of elliptic curves of rank *exactly* r. The only known r's are 0 and 1. For example in [BJK09], authors constructed infinitely many elliptic curves of rank exactly one. On the other hand, in [Mai93] Mai proves that under the parity conjecture, and if p and q are two primes such that $p - q = 24$, then the elliptic curves defined by an equation $x^3 + y^3 = 3pq$ have rank exactly two. However, we don't know that there are infinitely many such primes, though the celebrated work [Zha14] made a breakthrough.

In this chapter, we will show that the second condition of [Mai93] is not necessary, with the aid of Theorem 3.2. The main theorem of this chapter is following:

Theorem 5.1. *Assume the parity conjecture. Then, there are infinitely many elliptic curves whose Mordell–Weil group is exactly* $\mathbb{Z} \times \mathbb{Z}$.

5.2 Proof of the second application

As we did in Chapter 4, we call E_n by an elliptic curve defined by equation $x^3 + y^3 = nz^3$. Define $n' = -27n$ if 27 does not divide n, and $-n/27$ otherwise. Then there is an isogeny λ of degree 3 form E_n to $E_{n'}$ which is

$$\lambda(x,y) = \begin{cases} \left(\frac{x^4+4kxz^3}{x^3}, \frac{y(x^3-8k)}{x^3}\right), & \text{if } 27 \nmid k, \\ \left(\frac{x^4+4kx}{9x^3}, \frac{y(x^3-8k)}{27x^3}\right), & \text{if } 27 \mid k. \end{cases}$$

We will calculate a Selmer group of elliptic curve E_n and isogeny λ, which is denoted by $\mathrm{Sel}_\lambda(E_n/\mathbb{Q})$. (cf. Chapter 2.) We also define λ' be a dual isogeny of λ, and $\mathrm{Sel}_{\lambda'}(E_{n'}/\mathbb{Q})$ be a dual Selmer group. When

$$n = 3^\alpha \prod_{i=1}^{a} p_i \prod_{j=1}^{b} q_j,$$

be the prime decomposition of n such that $p_i \equiv 1 \pmod 3$ and $q_j \equiv 2 \pmod 3$, from [Sat86, Théorème 2.9], we have the following proposition.

Proposition 5.2. *If $n \equiv \pm 1 \pmod 9$, $p_i \equiv 1 \pmod 9$ for all i, $r_j \equiv -1 \pmod 9$ for all j, and for all $i = 1, \cdots, a$, l_k for $k = 1, \cdots, i-1, i+1, \cdots, a$ and r_j for $j = 1, \cdots, c$ are cubes modulo l_i, then $\mathrm{Sel}_\lambda(E_n/\mathbb{Q}) \cong (\mathbb{Z}/3\mathbb{Z})^{a+c}$ and $\mathrm{Sel}_{\lambda'}(E_{-27n}/\mathbb{Q}) \cong (\mathbb{Z}/3\mathbb{Z})^{a+1}$.*

Proof of Theorem 5.1. As in the proof of Proposition 4.6, we can construct elliptic curves whose rank is at least 1. By Lemma 4.4, an elliptic curve $E_{16b^6-a^2}$ has a rational point for some integer a and b. Theorem 3.2 shows that there are infinitely many integer b such that

$$8b^3 = p + 27q$$

for prime $p, q \equiv 1 \pmod 9$. When we define $a = p - 27q$, then

$$16b^6 - a^2 = (8b^3 + a)(8b^3 - a) = 27pq.$$

Since E_n and E_{27n} are isomorphic, $E_{16b^6-a^2} = E_{27pq}$ and E_{pq} have a nontrivial rational point. By Lemma 4.3 the rank of E_{pq} is at least 1, and by Lemma 4.5 the root number ω_{pq} is $+1$. So the parity conjecture implies that the rank of $E_{pq}(\mathbb{Q})$ is at least 2. Since $pq > 17$, $E_{pq}(\mathbb{Q})$ has no torsion points.

We use pq' instead of $(pq)'$. From the following exact sequences

$$0 \longrightarrow \frac{E_{pq'}(\mathbb{Q})[\lambda']}{\lambda(E_{pq}(\mathbb{Q}))[3]} \longrightarrow \frac{E_{pq'}(\mathbb{Q})}{\lambda(E_{pq}(\mathbb{Q}))} \longrightarrow \frac{E_{pq}(\mathbb{Q})}{3E_{pq}(\mathbb{Q})} \longrightarrow \frac{E_{pq}(\mathbb{Q})}{\lambda'(E_{pq'}(\mathbb{Q}))} \longrightarrow 0,$$

and

$$0 \longrightarrow \frac{E_{pq'}(\mathbb{Q})}{\lambda(E_{pq}(\mathbb{Q}))} \longrightarrow \mathrm{Sel}_{\lambda}(E_{pq}/\mathbb{Q}) \longrightarrow Ш(E_{pq}/\mathbb{Q})[\lambda] \longrightarrow 0,$$

$$0 \longrightarrow \frac{E_{pq}(\mathbb{Q})}{\lambda'(E_{pq'}(\mathbb{Q}))} \longrightarrow \mathrm{Sel}_{\lambda}\, E_{pq'}(\mathbb{Q}) \longrightarrow Ш(E_{pq'}/\mathbb{Q})[\lambda'] \longrightarrow 0,$$

we have that

$$\begin{aligned} \operatorname{rank} E_{pq}(\mathbb{Q}) &= \dim_{\mathbb{F}_3} \frac{E_{pq'}(\mathbb{Q})}{\lambda(E_{pq}(\mathbb{Q}))} + \dim_{\mathbb{F}_3} \frac{E_{pq}(\mathbb{Q})}{\lambda'(E_{pq'}(\mathbb{Q}))} - 1 \\ &\leq \dim_{\mathbb{F}_3} \mathrm{Sel}_{\lambda}(E_{pq}/\mathbb{Q}) + \dim_{\mathbb{F}_3} \mathrm{Sel}_{\lambda'}(E_{pq'}/\mathbb{Q}) - 1. \end{aligned}$$

Here we may assume $p \neq q$ for p, q since there is no b, p which satisfy $8b^3 = 28p$. By Proposition 5.2, we have

$$\mathrm{Sel}_{\lambda}(E_{pq}/\mathbb{Q}) \cong (\mathbb{Z}/3\mathbb{Z})^2, \qquad \mathrm{Sel}_{\lambda'}(E_{pq'}/\mathbb{Q}) \cong (\mathbb{Z}/3\mathbb{Z}),$$

so the rank of $E_{pq}(\mathbb{Q})$ is at most 2, which proves Theorem 5.1. □

We hope that we can prove the existence of infinitely many elliptic curves E whose Mordell–Weil groups are $\mathbb{Z} \times \mathbb{Z} \times T$ for some possible non-trivial torsion subgroups T, (cf. [Maz77]) in the near future.

Bibliography

[AK87] I. Allakov, É. Khamzaev, *Generalization of a theorem of Gallagher for the primes of an arithmetic progression*, Izv. Akad. Nauk UzSSR Ser. Fiz.-Mat. Nauk, **1** (1987) pp. 13 – 18. 22

[BCDT01] C. Breuil, B. Conrad, F. Diamond, R. Taylor, *On the modularity of elliptic curves over $\mathbb{Q}$: wild 3-adic exercises*, J. Amer. Math. Soc. **14** (2001) pp. 843 – 939. 10, 11

[Bob11] J. W. Bober, *Conditionally bounding analytic ranks of elliptic curves*, Proceedings of the Tenth Algorithmic Number Theory Symposium, Edited by E W. Howe and K. S. Kedlaya, (2013) pp. 135 – 144. 40

[BJ16] D. Byeon, K. Jeong, *Infinitely many elliptic curves of rank exactly two*, Proc. Japan Acad. Ser. A Math. Sci. **92** (2016) pp. 64 – 66. 2

[BJ17] D. Byeon, K. Jeong, *Sums of two rational cubes with many prime factors*, J. Number Theory, **179** (2017) pp. 240 – 255. 2

[BJK09] D. Byeon, D. Jeon, C. H. Kim, *Rank one quadratic twists of an infinite family of elliptic curves*, J. Reine Angew. Math. **633** (2009) pp. 67 – 76. 40

[BKW00] J. Brüdern, K. Kawada and T. D. Wooley, *Additive representation in thin sequences, II: The binary Goldbach problem*, Mathematika, **47** (2000), pp. 117 – 125. 5, 13, 14, 20, 21, 27, 31

[BP85] A. Balog and A. Perelli, *Exponential sums over primes in an arithmetic progression*, Proc. Amer. Math. Soc. **93** No.4 (1985) pp. 578 – 582. 16

[BS66] B. J. Birch and N. M. Stephens, *The parity of the rank of the Mordell-Weil group*, Topology **5** (1966), pp. 295 – 299. 11, 36

[Cas65] J. W. S. Cassels, *Arithmetic on curves of genus 1, VIII, On the conjectures of Birch and Swinnerton-Dyer*, J. Reine Angew. Math. **217** (1965), pp. 180 – 189. 6

[Con94] I. Connell, *Calculating root numbers of elliptic curves over* $\mathbb{Q}$, Manuscripta Math. **82**, (1994), pp. 93 – 104. 11

[Cow00] D. Coward, *Some sums of two rational cubes*, Q. J. Math. **51** (2000), pp. 451 – 464. 34

[CW77] J. Coates, A. Wiles, *On the conjecture of Birch and Swinnerton-Dyer*, Invent. Math. **39** (1977), pp. 223 – 251. 34

[Dav] H. Davenport, *Multiplicative number thoery*, Graduate Texts in Mathematics **74** Springer, 2000. 21

[DD11] T. Dokchitser, V. Dokchitser, *Root numbers and parity of ranks of elliptic curves*, J. Reine Angew. Math. **658** (2011), pp. 39 – 64. 12

[Duj1] A. Dejulla, *History of elliptic curves rank records*, available at https://web.math.pmf.unizg.hr/~duje/tors/rankhist.html 39

[Duj2] A. Dejulla, *High ranks elliptic curves with prescribed torsion*, available at https://web.math.pmf.unizg.hr/~duje/tors/tors.html 39

[Duj3] A. Dejulla, *Infinite families of elliptic curves with high rank and prescribed torsion*, available at https://web.math.pmf.unizg.hr/~duje/tors/generic.html 40

[DV09] S. Dasgupta, J. Voight, *Heegner points and Sylvester's conjecture*, Arithmetic Geometry, Clay Mathematics Proceeding, **8** (2009), pp. 91 – 102. 34

[FHS15] N. Freitas, B. V. Le Hung, S. Sikesk, *Elliptic curves over real quadratic fields are modular*, Invent. Math. **201** (2015), pp. 159 – 206. 10

[Gal70] P. X. Gallagher, *A large sieve density estimate near* $\sigma = 1$, Invent. Math. **11** (1970), pp. 329 – 339. 22

[GZ86] B. H. Gross, D. B. Zagier, *Heegner points and derivatives of L-series*, Invent. Math. **84** (1986), pp. 225 – 320. 11

[Har] R. Hartshorne, *Algebraic geometry*, Graduate Texts in Mathematics **52**, Springer, 2010. 6, 7

[Hel] H. A. Helfgott, *The ternary Goldbach problem*, available at https://arxiv.org/abs/1501.05438. 3

[IK] H. Iwaniec and E. Kowalski, *Analytic Number Theory*, American Mathematical Society, 2004. 16, 17, 18

[Kob] N. Koblitz, *Introduction to Elliptic Curves and Modular Forms*, Graduate Texts in Mathematics **97**, Springer, 1993. 6, 11

[Kol89] V. A. Kolyvagin, *Finiteness of* $E(\mathbb{Q})$ *and* $Ш(E, \mathbb{Q})$ *for a class of Weil curves*, Math. of the USSR Izvestiya, **32** (1989), pp. 523 – 542. 8, 11

[KSW16] Z. Klagsbrun, T. Sherman, J. Weigandt, *The Elkies curve has rank 28 subject only to GRH*, avilable at https://arxiv.org/pdf/1606.07178.pdf. 40

[Mai93] L. Mai, *The analytic rank of a family of elliptic curves*, Canadian J. of Math. **45** (1993), pp. 847 – 862. 35, 40

[Maz77] B. Mazur, *Modular curves and the Eisenstein ideal*, Publ. Math. Inst. Hautes Études Sci. **47** (1977), pp. 33 – 186. 8, 42

[Mes98] J. P. Mestre, *Rang de certaines familles de courbes elliptiques ́dinvariant donné*, Comptes Rendus de ÍAcadémie des Sciences - Series I - Mathematics, **327**, Issue 8, October 1998, pp. 763 – 764. 39

[MV75] H. L. Montgomery, R. C. Vaughan, *The exceptional set in Goldbach's problem*, Acta Arith. **27** (1975), pp. 353 – 370. 13, 22, 23, 24, 26, 27, 28, 30, 31

[Ner52] A. Néron, *Problémes arithmétiques et géométriques rattachés á la notion de rang d'une courbe algébrique dans un corps*, Bull. Soc. Math. France. **80** (1952), pp. 101 – 166. 39

[Per96] A. Perelli, *Goldbach numbers represented by polynomials*, Bibl. Rev. Mat. Iberoamericana, **12** (1996), pp. 349 – 361. 13

[Rub87] K. Rubin, *Tate–Shafarevich groups and L-functions of elliptic curves with complex multiplication*, Invent. Math. **89** (1987), pp. 527 – 560. 8

[Sat86] P. Satgé, *Groupes de Selmer et corps cubiques*, J. Number Theory, **23** (1986), pp. 294 – 317. 41

[Sat87] P. Satgé, *Un analogue du calcul de Heegner*, Invent. Math. **87** (1987), pp. 425 – 439. 33

[Sil94] J. H. Silverman, *Advanced topics in the arithmetic of elliptic curves*, Graduate Texts in Mathematics **151**, Springer, 1994. 6

[Sil09] ———————, *The arithmetic of elliptic curves*, second edition, Graduate Texts in Mathematics **106**, Springer, 2009. 6, 7, 9, 35

[SS] M. Schütt, T. Schioda, *Elliptic Surfaces*, Algebraic geometry in East Asia - Seoul 2008, Advanced Studies in Pure Mathematics **60** (2010), pp. 51 – 160. 39

[Sto] M. Stoll, *Descent on elliptic curves*, Panoramas et Synthèses **36**, Société Math. de France, 2012. 9

[Tia14] Y. Tian, *Congruent numbers and Heegner points*, Cambridge J. of Math. **2** (2014), pp. 117 – 161. 34

[Vau] R. C. Vaughan, *The Hardy-Littlewood Method (2nd edn.)*, Cambridge University Press, Cambridge, 1997. 3, 5

[Vin37] I. M. Vinogradov, *A new method in analytic number theory (Russian)*, Tr. Mosk. Mat. Obs. **10** (1937), pp. 5 – 122. 13

[Wil95] A. Wiles, *Modular elliptic curves and Fermat's last theorem*, Ann. Math. **141** (1995), pp. 443 – 551. 10

[Zha14] Y. Zhang, *Bounded gaps between primes*, Ann. Math. **179** (2014), pp. 1121 – 1174. 40

국문초록

이 논문에서는 타원 곡선의 정수점을 찾는 새로운 방법을 소개하고자 한다. 핵심적인 아이디어는 일차 다항식 형태로 일반화된 골드바흐 추측을 만족하지 않는 집합의 크기에 관한 이론을 공부하는 것으로 삼차꼬임이라고 불리우는 특정한 형태의 타원 곡선의 정수점을 찾을 수 있다는 것이다.

먼저 이전의 연구결과를 확장시켜, 특정한 일차식 형태로 일반화된 골드바흐 추측을 만족하지 않는 정수의 집합이 크지 않다는 것을 보인다. 그리고 이것이 어떻게 삼차꼬임 형태의 타원곡선의 정수점의 존재성을 보여주는지 설명한 뒤, 두 가지 응용을 보일 것이다. 첫 번째는 두 세제곱 유리수의 합으로 나타나면서 임의의 숫자의 소인수를 가지는 정수들이 무한히 많다는 것이고, 두 번째는 모델–베유 군이 정확하게 $\mathbb{Z} \times \mathbb{Z}$인 타원곡선이 무한히 많다는 것을 parity conjecture를 가정하면 증명할 수 있다는 것이다.

주요어휘: 타원곡선, 삼차꼬임, 모델–베유 군, 골드바흐 추측, 원 방법.
학번: 2012-20255